

AO 106 (Rev. 04/010) Application for Search Warrant

AUTHORIZED AND APPROVED/DATE:

*[Signature]* 12/9/21

## UNITED STATES DISTRICT COURT

for the  
WESTERN DISTRICT OF OKLAHOMAIN THE MATTER OF THE SEARCH OF  
**Motorola Cellular Phone, MC36F, IMEI:**  
**356892112291620**, CURRENTLY LOCATED  
AT 700 Colcord Drive, Oklahoma City Police  
Department)  
)  
)  
)  
)Case No: **MJ-21-691-STE**

## APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following Property:

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is:

- ☒ evidence of the crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section*

18 U.S.C. § 991(g)(1)

21 U.S.C. § 841(a)(1)

*Offense Description*

Possession of a Firearm After Felony Conviction

Possession of Controlled Substance with Intent  
to Distribute

The application is based on these facts:

See attached Affidavit of Task Force Officer Chris Grimes, ATF, which is incorporated by reference herein.

- ☐ Continued on the attached sheet(s).  
☐ Delayed notice of [No. of Days] days (give exact ending date if more than 30 days) is requested  
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

*[Signature]**Applicant's signature*CHRIS GRIMES, Task Force Officer  
Bureau of Alcohol, Tobacco, Firearms and Explosives

Sworn to before me and signed in my presence.

Date: **Dec 9, 2021**City and State: Oklahoma City, Oklahoma*[Signature]**Judge's signature*

SHON T. ERWIN, U.S. Magistrate Judge

*Printed name and title*

IN THE UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF  
**Motorola Cellular Phone, MC36F, IMEI:  
356892112291620**, CURRENTLY LOCATED  
AT 700 Colcord Drive, Oklahoma City Police  
Department

Case No. MJ-21-691-STE

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, ATF, Task Force Officer Chris Grimes, being first duly sworn, hereby depose and state  
as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal  
Rules of Criminal Procedure for a search warrant authorizing the examination of property—an  
electronic device—which is currently in law enforcement possession, and the extraction from  
that property of electronically stored information described in Attachment B.

2. I am a Task Force Officer with the Alcohol, Tobacco, Firearms and Explosives  
(ATF), and have been since October 1st, 2021. I have been employed as an Oklahoma City  
Police Officer since January 2008. Starting in July of 2008, I worked in the Hefner patrol  
division before transferring to the Santa Fe patrol division in April of 2009. I transferred to the  
Oklahoma City Police Department (OCPD) Gang Enforcement Unit in September 2012. I  
promoted to Detective in April of 2015 where my current title is Investigator in the Violent  
Crimes Unit.

3. I received formal training and instruction in the detection, recognition, and uses of several different types of illegal narcotics from the Police Academy and OCPD. Since my graduation from the basic Police Academy, I have attended schools and seminars concerning the manufacturing and trafficking of narcotics and dangerous drugs. I have attended schools sponsored by the Oklahoma City Police Department, the Council on Law Enforcement Education and Training (CLEET), Oklahoma Gang Investigators Association, and Chicago Gang Investigators Association.

4. I have assisted in numerous investigations involving city, state, and federal prosecutions, which have resulted in apprehension of persons on narcotic related charges, weapons, and assault charges as well as the seizure of drugs, property, and monies. I have had conversations with and been in the company of other experienced local, state, and federal law enforcement officers as well as prosecuting attorneys representing both state and federal systems concerning narcotics and dangerous drug trafficking activities and other criminal violations including weapons charges and felony and misdemeanor assaults. Through my involvement in past investigations, I have become familiar with the clandestine business practices of drug traffickers, gang members and the criminal activity of gang members such as shootings, assaults, robberies, burglaries, and other felony crimes associated with gang members.

5. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachment A** of this Affidavit for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 991(g)(1) (Possession of a Firearm After Felony Conviction) and Title 21, United States Code, Section 841(a)(1) (Possession of Controlled Substance with

Intent to Distribute). This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

**IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

6. The property to be searched is a **Motorola Cellular Phone, MC36F, IMEI: 356892112291620** hereinafter the “Device.” The Device is currently located at 700 Colcord Drive, the Oklahoma City Police Department Headquarters in the Western District of Oklahoma.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in **Attachment B**.

**PROBABLE CAUSE**

8. On 10/27/2021, Weatherford Police Department responded to a call for service at 407 East Franklin Avenue in Weatherford Oklahoma, Custer County, in the Western District of Oklahoma (Weatherford residence). During the call Weatherford Police Officers found S.P. unconscious, suffering from an apparent fentanyl overdose. S.P. was the live-in girlfriend of **IAN BRAND (BRAND)**, both of whom lived at the Weatherford residence. Officers learned **BRAND** fled the scene when the 911 call was placed. After S.P. was transported from the residence, Weatherford Police Officers obtained and executed a search warrant for the Weatherford residence. During the search, officers located two firearms, live ammunition, and drug paraphernalia. Weatherford Police Officers knew **BRAND** was a convicted felon and learned he possibly fled the scene with a large amount of Fentanyl narcotics. Based on the evidence located during the search warrant, Weather Police issued an arrest warrant for **BRAND** for two counts of Possession of a Firearm After Former Conviction of a Felony. Examination of both firearms

revealed neither were manufactured in the state of Oklahoma, meaning both crossed state lines to reach Oklahoma. At the time, **BRAND** also had a pending warrant out of Oklahoma County for Possession of a Firearm After Former Conviction of a Felony.

9. During the execution of the search warrant of the Weatherford residence, officers located a cell phone, identified as the “first phone,” belonging to **BRAND**. As part of their investigation into the state charges, Weatherford officers obtained and executed a search warrant on the first phone. Evidence from the search of **BRAND**’s first phone shows **BRAND** using text and instant messaging, dating to back to at least August 4, 2021, to facilitate purchasing and selling firearms and illegal narcotics. These messages indicate **BRAND** frequently traveled between Weatherford and Oklahoma City, both in the Western District of Oklahoma, to conduct narcotics transactions. The first phone also contains videos of individuals portioning out illegal narcotics into what appears to be, both through visual inspections and based on conversations of the individuals, one-ounce baggies. Photographs located on the first phone support a conclusion that **BRAND** is one of the individuals in said videos. Other photographs show **BRAND** possessing firearms, some of which were recovered from both the Weatherford residence and from a subsequent search which will be detailed below. In messages located on the first phone, **BRAND** acknowledges the fact that he possesses another phone. The evidence found on **BRAND**’s first phone demonstrate that he uses his cellular devices to aid and facilitate his criminal acts.

10. Weatherford officers received information from S.P.’s family that **BRAND** fled to his sister’s home, located in the Village, Oklahoma City, Oklahoma. On 11/02/2021, Weatherford officers reached out to members of the OCPD Violent Crimes Investigations Unit

(VCI) and the Violent Crimes Apprehension Team (VCAT) to request assistance in locating and apprehending **BRAND**. VCI and VCAT officers were able to locate **BRAND** at his sister's, Sarah Brand's, residence located at 1916 Westchester Drive, Village Oklahoma, in the Western District of Oklahoma (Village residence). Members of the VCAT Unit are also cross deputized with the Oklahoma County Sheriff Office, giving them jurisdiction to conduct investigations in the Village. The VCAT officers were also assisted by the Village Police Department during this arrest incident. Investigators with the VCI assisted in the investigation of new charges during his arrest.

11. During the arrest incident, Sarah Brand consented to a search of the Village residence by OCPD and Village officers. Sarah Brand read and signed a search wavier prior to the search being conducted. During the search of the residence, officers located three additional firearms, live ammunition, gun magazines, ballistic vest, and a Motorola cellular phone. Examination of the additional firearms revealed none were manufactured in the state of Oklahoma, meaning both crossed state lines to reach Oklahoma. Although officers did attempt to determine who the cellular phone belonged to, they were unable to do so during the initial investigation.

12. During this investigation, I reviewed a recorded Oklahoma County Jail call placed on 11/02/2021 to a female during which **BRAND** confirms the Motorola cell phone was in fact his personal phone at the time of arrest. During the call, **BRAND** gives the unlock code to the Motorola taken into custody during his arrest. During the recorded phone call, **BRAND** also admits to possessing multiple firearms while being prohibited as a convicted felon, thus a prohibited person.



13. The Device is currently in the lawful possession of the Oklahoma City Police Department. It came into the Oklahoma City Police Department's possession during **BRAND's** fugitive arrest and subsequent consensual search of the Village residence. Therefore, while the Oklahoma City Police Department might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

14. The Device is currently in the VCI office, which is a secured office within a secured facility. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the Oklahoma City Police Department.

#### **TECHNICAL TERMS**

15. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and

from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include:

- b. storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- c. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved



in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

16. Based on my training and experience, I know examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggest who possessed or used the device. I further know these Cell Phone devices have capabilities that allow them to serve as wireless telephones, digital cameras, GPS navigation devices and Internet Devices. Furthermore, based on my knowledge of the initial Weatherford investigation, I know evidence from the search of **BRAND**’s first phone shows **BRAND** buying, selling, and possessing firearms along with him selling illegal narcotics. Evidence recovered by law enforcement demonstrates he uses his cellular devices to aid, facilitate, and document his criminal acts.

**ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

17. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

18. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

19. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

20. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

21. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.
- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
- c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a

facial recognition feature called “Face ID.” During the Face ID registration process, the user holds the device in front of his or her face. The device’s camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

- d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.
- f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers,

that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

- g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a

user of the device, to unlock the device using biometric features in the same manner as discussed above.

- h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

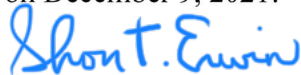
**CONCLUSION**

22. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted

  
Chris Grimes  
Task Force Officer, ATF

Subscribed and sworn to before me  
on December 9, 2021:



UNITED STATES MAGISTRATE JUDGE



**ATTACHMENT A**

The property to be searched is a **Motorola Cellular Phone, MC36F, IMEI: 356892112291620** hereinafter the “Device.” The Device is currently located at 700 Colcord Drive, the Oklahoma City Police Department Headquarters.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

1. All records on the Device described in Attachment A that relate to violations of **18 U.S.C § 922(g)(1)** and **21 U.S.C § 841(a)(1)** which involve **BRAND** including:

- a. any and all records related to the purchasing, selling, or possession of illegal narcotics;
- b. any and all records related to the purchasing, selling, or possession of firearms;
- c. contact information of individuals identified as narcotics or firearms customers and related identifying information;
- d. any records regarding **BRAND**'s location data beginning August 4, 2021, until November 2, 2021;

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

As used above, the terms “records” and “information” include all foregoing items of evidence in whatever form and by whatever means they may have been created.